



WHITEPAPER
**Segurança da Rede Elétrica
Inteligente
Mitos vs. Realidade**

Entendendo Ameaças e Como Combatê-las

Construir a rede elétrica inteligente exige uma plataforma de rede unificada para interconectar todos os dispositivos dentro da infraestrutura de energia elétrica. Com base no Protocolo de Internet (IP), essa infraestrutura de rede conecta medidores e subestações a centros de operações e fornece suporte a funções de controle e gerenciamento, bem como aplicativos de rede elétrica inteligente, como a infraestrutura de medição avançada (AMI).

Pode haver prejuízos significativos se um ataque malicioso na rede ou uma configuração incorreta acidental causar defeitos à rede elétrica inteligente. Pela função crucial da rede dentro da rede elétrica inteligente, empresas de serviços públicos essenciais, reguladores e outras partes interessadas dentro do setor de energia elétrica estão compreensivelmente preocupados com sua segurança. Infelizmente, uma variedade de mitos sobre a segurança da rede elétrica inteligente surgiu, causando alarme e confusão desnecessários e desacreditação de uma discussão de ameaças de segurança legítimas e das tecnologias disponíveis para combatê-las.

Este artigo desmarcará os mitos de segurança mais comuns sobre a rede elétrica inteligente, fornece uma visão geral das tecnologias de segurança estabelecidas e destaca como essas tecnologias podem ser usadas para contrapor ameaças reais à rede elétrica inteligente.

Mitos de Segurança da Rede Elétrica Inteligente

Mito nº 1: ninguém está prestando atenção à segurança.

Uma pesquisa de provedores de empresas de serviços públicos essenciais que entraram em projetos de rede elétrica inteligente revela que todos eles estão integrando segurança à infraestrutura. Da mesma forma, fornecedores de tecnologia da rede elétrica inteligente estão implementando vários padrões e mecanismos de segurança dentro dos seus produtos, realizando análise de ameaça e testes de penetração em seus sistemas e ajudando os clientes das empresas de serviços públicos essenciais a verificar arquiteturas de segurança. Órgãos regulamentadores, como o National Institute of Standards and Technology (NIST), a North American Electric Reliability Corporation (NERC) e outros, estão ativamente trabalhando com todas as partes interessadas para definir os padrões de segurança comuns do setor para redes de rede elétrica inteligente.

Mito nº 2: a rede elétrica inteligente torna fácil para hackers causar apagões disseminados.

A rede elétrica inteligente é projetada para vincular vários dispositivos para facilitar o gerenciamento e o controle operacional. Essa arquitetura na verdade torna mais fácil implementar uma variedade de verificações, limites e restrições em vários pontos ao longo da rede. Por exemplo, restrições físicas no centro de operações podem ser combinadas com a inteligência em cada dispositivo em campo para verificar a autorização adequada antes de um comando crítico para o todo o sistema, como uma desconexão remota, possa ser executado. Os operadores da rede elétrica inteligente podem reduzir drasticamente a ameaça de um apagão disseminado assumindo uma abordagem em camadas à segurança de rede que inclua conectividade de segurança, segurança de perímetro e serviços de identidade e autorização e usando hardware de segurança de rede dedicado, ferramentas de software e políticas de gerenciamento de segurança eficazes.

Mito nº 3: usar IP na rede de comunicações de dados significa que a rede elétrica inteligente é tão vulnerável quanto a Internet.

A Internet é uma rede pública, aberta a qualquer um e a todos. Em contraste, muitas redes baseadas em IP, incluindo aquelas nas implementações da rede elétrica inteligente, são privadas e não estão conectadas à Internet pública. Usado pela primeira vez nos anos 1970, o IP é um pacote de protocolo maduro e robusto que oferece vários mecanismos de segurança. Redes de IP privadas são protegidas ainda por segurança de camada de link, criptografia de rede e fortes controles de autorização e autenticação. Como resultado, várias empresas privadas, instituições do governo e militares ao redor do mundo contam com redes IP privadas para fornecer comunicações seguras para todas as suas aplicações críticas para a missão e altamente confidenciais.

Mito nº 4: redes sem fio carecem de segurança e são fáceis de invadir.

Usuários sem fio enfrentam uma ameaça principal: ter seus dados confidenciais interceptados durante a transmissão. Redes sem fio podem ser protegidas por vários meios, sendo que a maioria deles utiliza os dois conceitos fundamentais de autenticação de usuários e dispositivos e criptografia de dados. O nível de segurança implementado é geralmente conduzido pelas necessidades dos aplicativos que estão acessando a rede sem fio; ler um medidor por um dispositivo portátil sem fio exigiria uma segurança menos rígida que atualizar esse medidor, por exemplo. Técnicas de segurança sem fio foram comprovadas como sendo muito eficientes quando aplicadas de maneira consistente em toda a rede e acopladas com medidas para garantir que uma violação individual, se ocorrer, tenha um impacto apenas localizado.

Mito nº 5: violar um medidor fornece acesso à toda a rede inteligente, pois tudo está interconectado.

Uma das primeiras considerações de segurança para a rede elétrica inteligente é converter ataques em massa, que colocam todo o sistema em risco, em ataques de pequena escala, que estão limitados a um escopo muito reduzido. Ataques em massa podem ser interrompidos aplicando técnicas de segurança a cada etapa de um processo, incluindo exigir que várias partes trabalhem juntas para ativar uma dada função; por exemplo, dois operadores devem trabalhar de maneira combinada para iniciar comandos para todo o sistema (isso é conhecido como “controle por duas partes”). Além disso, os medidores e outros dispositivos de rede podem ser projetados de modo que cada um tenha uma identidade exclusiva e comunique-se com outros dispositivos apenas depois de cada um ter verificado a identidade do outro.

Mito nº 6: esquemas de segurança proprietários são mais seguros que tecnologias de segurança baseadas em IP.

Soluções de segurança proprietárias são essencialmente sistemas fechados, desenvolvidos e mantidos por um único fornecedor. Como consequência, a robustez das soluções proprietárias depende do conhecimento de um número limitado de indivíduos empregados por esse fornecedor e do conhecimento obtido a partir de um número limitado de implementações. As soluções de segurança proprietárias frequentemente dependem de manter certos aspectos em segredo que, quando descobertos, levam a um total colapso da segurança do sistema.

Em contraste, tecnologias de segurança baseadas em IP foram desenvolvidas coletivamente pelas melhores mentes de segurança no mundo todo e fortalecidas ao longo de décadas de uso mundial contra uma ampla variedade de ataques. Porque são padronizados, os mecanismos de segurança baseados em IP podem ser usados com uma ampla variedade de hardwares e softwares de diversos fornecedores. Além disso, tecnologias de segurança baseadas em IP têm comprovadamente alta capacidade de escala.

Fundamentos de Segurança

Uma ampla variedade de mecanismos de segurança foi desenvolvida dentro dos setores de computador e rede, muitos dos quais estão na terceira ou quarta geração. Tecnologias de segurança baseadas em IP, por exemplo, são bem estabelecidas e fortalecidas em campo, e muitas foram padronizadas.

Mecanismos de segurança podem ser usados para controlar quem e o que acessou a rede elétrica inteligente e que ações podem ser realizadas. Também podem determinar se as informações enviadas pela rede originam-se da fonte declarada e chegam inalteradas. Além da tecnologia, a segurança envolve políticas e práticas. Por exemplo, uma empresa de serviços públicos essenciais que restringe quem pode fazer alterações em todo o sistema ou pode exigir controle de duas partes para operações críticas. Uma boa plataforma de rede elétrica inteligente fornece às empresas de serviços públicos essenciais as ferramentas de que precisam para implementar com segurança essas políticas.

A lista a seguir inclui as tecnologias de segurança de rede mais usadas.

Autenticação é o processo de garantir que os usuários e dispositivos na rede sejam aqueles que afirmam ser. A autenticação conta com credenciais que variam do nome de usuário e senha básicos ao uso de certificados e assinaturas digitais como uma maneira de estabelecer uma identidade do usuário. Certificados digitais fornecem informações sobre a identidade de uma entidade, junto com outras informações, e são emitidos por uma autoridade de certificação que garante a validade das informações no certificado. Uma assinatura digital é um esquema matemático para demonstrar a autenticidade de uma mensagem ou documento digital. Assinaturas digitais são comumente usadas para distribuição de software, transações financeiras e em outros casos em que é importante detectar adulteração ou fraude.

Para mais segurança, dois ou mais fatores podem ser necessários para autenticação. A autenticação de dois fatores normalmente combina algo que o usuário sabe (como uma senha) com algo que o usuário tem (como um cartão de chave, impressão digital ou outro token de segurança).

A **Autorização** concede a usuários e dispositivos o direito de acessar recursos e realizar as ações especificadas. Como parte da autorização, os usuários e dispositivos podem ter funções atribuídas, por exemplo, que deem a eles um conjunto de privilégios. Definindo o escopo de o que um usuário ou dispositivo autenticado pode fazer, certificados digitais podem ser usados como um mecanismo de autorização.

Mecanismos de controle de admissão de rede limitam o acesso à rede a usuários e dispositivos autenticados e autorizados. Abordagens para aplicar controle de admissão de rede incluem firewalls e endereçamento privado, e frequentemente estende-se a controle baseado em função, que restringe as atividades permitidas de um dado usuário com base na sua função dentro da organização.

Criptografia garante a confidencialidade dos dados usando um algoritmo (chamado de cifra) para transformar os dados e torná-los ilegíveis a qualquer um, exceto aqueles de posse de informações especiais, normalmente referidas como chave. Ambas as “pontas” da transação precisam da chave para poderem enviar e ler as informações enquanto protegem sua confidencialidade durante a transmissão. A força da proteção depende da natureza do algoritmo de criptografia e da extensão da chave; quanto mais longa for a chave, mais seguros estão os dados que ela criptografa. Por exemplo, o Advanced Encryption Standard (AES) tem um algoritmo mais sofisticado e uma extensão de chave mais longa, então ele supera o Digital Encryption Standard (DES) anterior.

Mecanismos de verificação de **Integridade** são projetados para detectar alterações não autorizadas ao conteúdo da mensagem. Um mecanismo é o hash digital, pelo qual o dispositivo de envio calcula uma soma de verificação criptográfica sobre a mensagem original. O dispositivo de recebimento realiza a mesma função de hash na mensagem e a compara com o original. Se o conteúdo tiver sido alterado em trânsito, os valores de hash são diferentes e o conteúdo é rejeitado.

Hash pode ser combinado com chaves para maior garantia de integridade. Por exemplo, o computador de envio usa uma função de hash e uma chave compartilhada para calcular a checksum para a mensagem e a inclui com os dados. O computador de recebimento realiza a mesma função de hash na mensagem recebida e na chave compartilhada e a compara com o original. Porque uma chave é usada, tanto a integridade quanto a autenticidade de dados de uma mensagem são verificados.

Alerta notifica a equipe ou outros sistemas sobre ataques em potencial ou comprometimentos de segurança para que possam agir. Os dispositivos podem ser configurados para enviar alertas quando detectam acesso não autorizado, falhas de verificação de integridade ou outras condições anômalas que podem indicar a ocorrência de uma falha de segurança ou incidente.

Auditoria fornece registros de todas as atividades na rede, permitindo revisão independente. Por exemplo, redes da rede elétrica inteligente devem registrar e fornecer um carimbo de hora em todas as atividades, incluindo o originador de uma ação e o resultado dessa ação.

Ameaças à Rede Elétrica Inteligente

Ameaças à rede elétrica inteligente podem ser classificadas em três grupos amplos: ameaças no nível do sistema que tentam derrubar a rede elétrica; tentativas de roubar serviço elétrico e tentativas de comprometer a confidencialidade dos dados no sistema.

Frequentemente presume-se que ameaças de segurança vêm exclusivamente de hackers e outros indivíduos ou grupos externos com intenção maliciosa. Porém, o pessoal da empresa de serviços públicos essenciais e outras partes internas também impõem um risco, pois eles têm acesso autorizado a uma ou mais partes do sistema. Partes internas conhecem as informações, como senhas armazenadas nos bancos de dados do sistema, e têm acesso ao perímetro protegido, chaves de criptografia e outros mecanismos de segurança que são alvos de comprometimentos. E nem todas as violações de segurança são maliciosas; algumas resultam de configurações incorretas acidentais, falha em seguir procedimentos e outros descuidos.

Ao analisar a lista de ameaças abaixo, tenha em mente que os perpetradores podem ser partes internas ou externas. Além das mitigações listadas, as empresas de serviços públicos essenciais também devem empregar melhores práticas operacionais, incluindo a aplicação de controles sobre o acesso físico a componentes do sistema de comunicação, bem como políticas e procedimentos rígidos de gerenciamento de mudança do sistema que apliquem controles sobre modificações do sistema.

Ameaças no nível do sistema

A meta de ameaças no nível do sistema é derrubar parte ou toda a rede elétrica inteligente negando aos operadores acesso ao campo de rádio, ao espectro de RF, a rádios individuais ou Módulos de Comunicação com medidores. Por exemplo, entidades ou indivíduos com intenção maliciosa podem tentar mudar as instruções programadas no medidor, alterar os limites de alarme ou emitir comandos não autorizados aos medidores ou outros dispositivos de controle na rede elétrica inteligente. Essas ações podem resultar em danos ao equipamento, desligamento prematuro de energia ou processos ou mesmo desativar o equipamento de controle. As ameaças no nível do sistema incluem:

- » **Subversão ou tomada de controle de rádio:** essa ameaça é caracterizada por uma tentativa de assumir o controle de um ou mais rádios ou Módulos de Comunicações de RF nos medidos, de modo que “pertencam” aos responsáveis pelo ataque. A ameaça mais comum nessa categoria é a substituição de firmware; os responsáveis pelo ataque tentam inserir firmware modificado em um dispositivo e/ou tentam disseminar firmware comprometido a vários dispositivos.
 - *Mitigação:* antes de executar o firmware, os Módulos de Comunicações usam chaves criptográficas e assinaturas digitais para confirmar se o firmware é de uma origem autenticada e não foi modificado.
- » **Invasão da rede por estranhos:** essas ameaças vêm de rádios “estranhos” tentando unir-se à rede RF ou impedindo que os Módulos de Comunicações comuniquem-se de maneira adequada. Por exemplo, um invasor pode tentar usar os Módulos de Comunicação para dar carona a tráfego não autorizado na rede, tentar impedir os Módulos de Comunicação de enviar ou receber tráfego ou usar um rádio “estranho” para interceptar e/ou substituir o tráfego. Além disso, um invasor pode tentar modificar as credenciais de um rádio ou de Módulos de Comunicações para que assumam uma função diferente.
 - *Mitigação:* a inserção ou adulteração de dados pode ser evitada através do uso de criptografia e verificação de integridade; mecanismos de autenticação podem garantir que rádios “estranhos” sejam isolados, uma vez que nenhum Módulo de Comunicações ou rádio na rede da rede elétrica inteligente se comunicará com um dispositivo não autenticado. Além disso, empregar mecanismos de proteção de dados para credenciais.

» **Negação de Serviço:** essas ameaças resultam em toda ou parte da rede tornar-se inutilizável. Elas incluem buracos negros de roteamento, pelos quais é feito o hack de um nó de modo que ele é divulgado como o caminho mais curto para qualquer lugar, resultando em todo o tráfego ser direcionado para ele; congestionamento de espectro de RF, que impede que o sinal seja recebido; jabbering, pelo qual um nó legítimo é capturado para enviar tanto tráfego que os outros nós não podem se comunicar; kill packets, que são pacotes de protocolo que fazem os rádios falharem ou tornarem-se inalcançáveis via o campo de RF; stack smashing, um método de subverter ou desativar o sistema operacional de um dispositivo ou aplicativo sobrecarregando os buffers de memória de modo que os dados sejam expostos, perdidos ou corrompidos; ataques sobre o sistema de criptografia ou os protocolos que resultam na penetração ou degradação do sistema; e ataques ambientais, em que um serviço é interrompido devido a danos físicos, clima adverso ou desastres naturais.

- *Mitigação:* autenticação, criptografia, uso de certificados e verificação de integridade podem combater os buracos negros de roteamento, os kill packets e o jabbering no nível de protocolo. Congestionamento de espectro de RF e jabbering no nível de RF são combatidos usando o Frequency-Hopping Spread Spectrum (FHSS), que muda o canal de 50 a 100 vezes por segundo, tornando difícil de bloquear. A ameaça imposta por um stack smashing pode ser mitigada implementando dispositivos cujo software foi rigorosamente projetado e testado

Ataques criptográficos são raros, mas podem ser encontrados através do uso de fortes algoritmos de criptografia. Para dispositivos como medidores que são feitos para estarem em campo por 20 anos, implemente algoritmos classificados para serem seguros por mais de 20 anos. De maneira similar, para suportar ameaças ambientais, implemente dispositivos de comunicações que sejam resistentes a adulterações e resistam aos padrões industriais e militares para fatores ambientais, como temperatura, umidade e raios.

» **Comprometimento de credencial:** credenciais provam a identidade de uma entidade no sistema e concedem a essa entidade acesso à rede de comunicações, incluindo pontos de acesso (APs), Módulos de Comunicações/medidores e operações e sistemas de gerenciamento. O comprometimento de credenciais permite ao responsável pelo ataque acessar o sistema de comunicação para qualquer fim, como negação ou roubo do serviço.

- *Mitigação:* a autenticação criptográfica combinada com mecanismos de proteção para dados em repouso pode combater o comprometimento de credenciais garantindo que as credenciais sejam confidenciais e a comunicação possa ocorrer apenas entre componentes autenticados e confiáveis.

» **Comprometimento das funções administrativas:** se indivíduos não autorizados obtiverem acesso ao banco de dados de gerenciamento da rede elétrica inteligente, eles podem desativar toda a rede. Da mesma forma, com acesso ao banco de dados que armazena dados privilegiados, um invasor poderia alterar as credenciais para quais rádios respondem e potencialmente desativar toda a rede. Similarmente, acesso não autorizado a faturamento e outros sistemas de tarefas administrativas abriria uma porta para roubo de serviço, bem como comprometimento da privacidade do cliente.

- *Mitigação:* segurança física, autenticação forte, autorização usando privilégios baseados em função e controle de acesso à rede usando firewalls são todos mecanismos que podem ser usados para combater o comprometimento das funções administrativas. Além disso, todas as informações confidenciais, incluindo senhas, devem ser criptografadas no banco de dados. Conexões a bancos de dados sensíveis devem ser criptografadas também. Acesso ao sistema de controle deve ser limitado a locais fisicamente protegidos específicos. Autenticação de dois fatores deve ser usada para todos os operadores autorizados e controles de duas partes devem ser usados para as operações mais importantes, incluindo atribuições e alterações de privilégios. Além disso, módulos de segurança de hardware com limitação de taxa podem aumentar o controle sobre operações sensíveis, como desconexões remotas de medidores.

Roubo de Serviço

Além de ataques em potencial à rede elétrica inteligente em si, as empresas de serviços públicos essenciais enfrentam ameaças que podem resultar em roubo de serviço e impedir o operador de coletar receita. Por exemplo, medidores individuais ou grupos de medidores podem ser subvertidos para relatar incorretamente o cliente, a quantidade de serviço fornecida ou o custo do serviço fornecido (mudando de uma camada de preço superior para uma de preço inferior). Ameaças nessa categoria incluem:

- » **Clonagem:** com a clonagem, um invasor poderia substituir um ID de medidor ou rádio por um duplicado projetado para relatar uso zero.
 - *Mitigação:* combate à clonagem com autenticação e emprego de mecanismos de proteção de dados para credenciais.
- » **Migração:** para reduzir o uso relatado e as faturas associadas, um invasor trocaria um medidor (ou seu Módulo de Comunicações) de um local relatando alto uso por um medidor/Módulo de Comunicações de um local relatando baixo uso.
 - *Mitigação:* a autenticação e o uso de verificação de credenciais mitigam riscos de migração, especialmente se os operadores vincularem a credencial do medidor a uma área regional ou mesmo a um endereço específico. Além disso, alguns medidores da rede elétrica inteligente são projetados para enviar “alertas de adulteração” caso ocorra uma desativação suspeita.
- » **Intrusão na interface do Módulo de Comunicações/Medidor:** o Módulo de Comunicações dentro de cada medidor está conectado ao medidor via uma porta serial, que pode ser desconectada de modo que o medidor não relate o uso. Como alternativa, um invasor pode tentar invadir o Módulo de Comunicações para alterar as informações de uso.
 - *Mitigação:* roubo de serviço via intrusão de interface do medidor/Módulo de Comunicações pode ser mitigado implementando medidores inteligentes capazes de detectar essas desconexões e outros tipos de adulteração e relatório, como incidentes a operadores. O uso de credenciais criptográficas e o requisito de autenticação antes de qualquer tipo de comunicação com o Módulo de Comunicações frustra ataques ao Módulo de Comunicações em si.

Ameaças à privacidade/confidencialidade

Alguns ataques do sistema podem resultar na exposição de informações que identificam pessoas. Essas ameaças à confidencialidade incluem:

- » **Intercepção de RF:** espionagem passiva na rede de rádio poderia permitir a um invasor capturar pacotes.
 - *Mitigação:* a segurança inerente do FHSS combate essa ameaça, enquanto a criptografia de dados adiciona outra camada de proteção da confidencialidade.
- » **Comprometimento do ponto de encaminhamento:** informações confidenciais podem ser expostas se um nó na rede for comprometido de modo que encaminhe tráfego para um indivíduo ou entidade não autorizado.
 - *Mitigação:* Essa ameaça pode ser combatida com o uso de dispositivos resistentes a adulteração capazes de enviar alertas de adulteração; com o uso de criptografia; e com a implementação de dispositivos que armazenam com segurança chaves criptográficas e realizam uma verificação de autenticação em cada link estabelecido.
- » **Intercepção de rede IP de backhaul:** informações podem ser interceptadas conforme percorrem a rede de backhaul.
 - *Mitigação:* apenas entidades autenticadas podem enviar tráfego sobre a rede de backhaul e esses dados são enviados dentro de túneis protegidos usando protocolos de Segurança IP (IPsec).

- » **Comprometimento de medidor:** qualquer ameaça à privacidade relacionada ao comprometimento físico de um medidor.
 - *Mitigação:* essa ameaça pode ser combatida usando as mesmas técnicas para frustrar um comprometimento de ponto de encaminhamento.

A Perspectiva da Silver Spring

A Silver Spring projetou segurança em cada elemento da sua Smart Energy Platform (Plataforma de energia inteligente). A plataforma une rede, software e serviços para entregar o escopo completo de aplicativos de rede elétrica inteligente. A rede aberta de autoconfigurada da empresa, os aplicativos de funções administrativas integrados e os amplos serviços profissionais permitem às empresas de serviços públicos essenciais implementar de maneira rápida e eficiente medição avançada, comunicações para automação de distribuição, resposta à demanda, integração de rede de área doméstica e lar inteligentes e veículos elétricos.

Desde o início, a Silver Spring reconheceu que a rede elétrica inteligente pode ser alvo de atividade maliciosa, e entendeu as vulnerabilidades apresentadas pelos dispositivos de interconexão. Como consequência, a empresa assumiu uma abordagem de arquitetura à segurança e a integrou através dos dispositivos de hardware, operações de software e transações no nível da rede executando através da infraestrutura da rede elétrica inteligente.

E porque tanto as demandas funcionais sobre a rede elétrica quanto o panorama de ameaças em torno dela evoluem com o tempo, a Silver Spring projetou capacidade de atualização segura no sistema. Como resultado, os clientes da empresa de serviços públicos essenciais podem aumentar a funcionalidade da rede elétrica inteligente, bem como a segurança através de atualizações pelo ar a hardware e software da Smart Energy Platform (Plataforma de energia inteligente).

Segurança é um imperativo em qualquer implementação de rede elétrica inteligente, e a Silver Spring aprecia a oportunidade de discutir suas técnicas de segurança específicas em mais detalhes.

Sobre a Silver Spring Networks

A Silver Spring Networks é uma fornecedora de soluções de smart grid que permite às concessionárias de serviços públicos obter eficiência operacional, reduzir as emissões de carbono e dar poder a seus clientes, com novos modelos para monitorar e gerenciar o seu consumo de energia. A Silver Spring fornece hardware, software e serviços que permitem às concessionárias implantar e executar várias soluções de smart grid, incluindo Medição avançada, Resposta à demanda, Automação da distribuição e Geração distribuída em uma única rede unificada. A Smart Energy Platform (Plataforma de energia inteligente) da Silver Spring se baseia em padrões de Internet Protocol (IPv6), permitindo a comunicação bidirecional contínua entre a concessionária de serviços públicos e os dispositivos da rede. A Silver Spring tem várias implantações com concessionárias líderes em todo o mundo, incluindo Baltimore Gas & Electric, CitiPower & Powercor, Florida Power & Light, Jemena Electricity Networks Limited, Pacific Gas & Electric, Pepco Holdings, Inc., United Energy Distribution, entre outras. Para obter mais informações, visite www.silverspringnet.com.

Copyright © 2011 Silver Spring Networks. Todos os direitos reservados.
Todas as marcas comerciais pertencem a seus respectivos proprietários. Rev. 9/8/11

Sede corporativa
555 Broadway Street
Redwood City, CA 94063
650.298.4200 Telefone
866.204.0200 Ligação gratuita