EXHIBIT 2

Junos® OS

Authentication and Integrated User Firewalls Feature Guide for Security Devices

Modified: 2017-08-02

certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

Figure 1 on page 12 depicts how SSL inspection (on an existing SRX Series IDP module) is typically used to protect servers. SSL inspection requires access to the private keys used by the servers so that the SRX Series device can decrypt the encrypted traffic.

Figure 1: SSL Inspection on an Existing SRX Series IDP Module

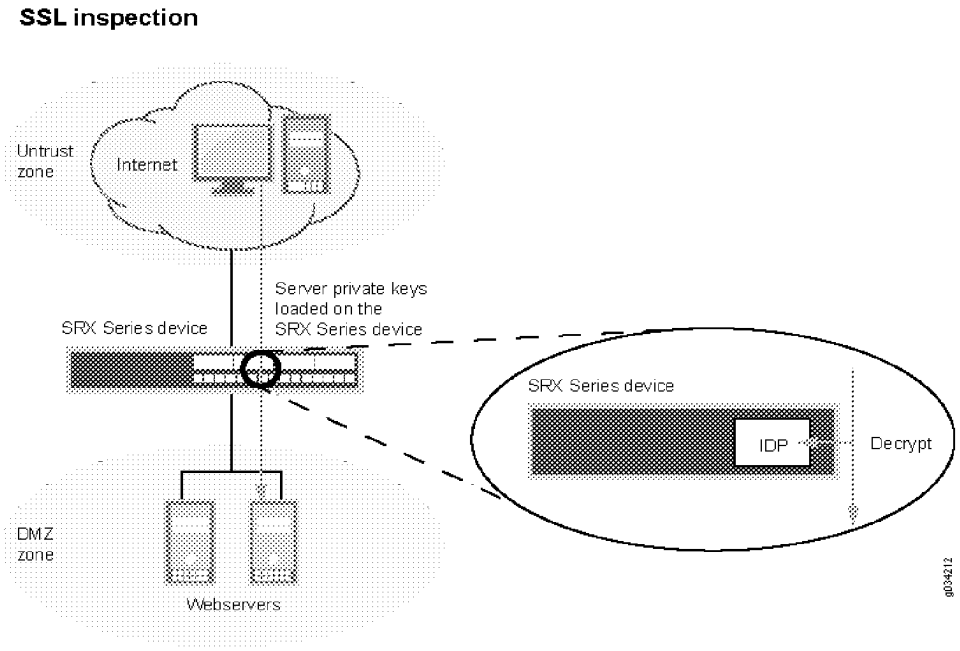


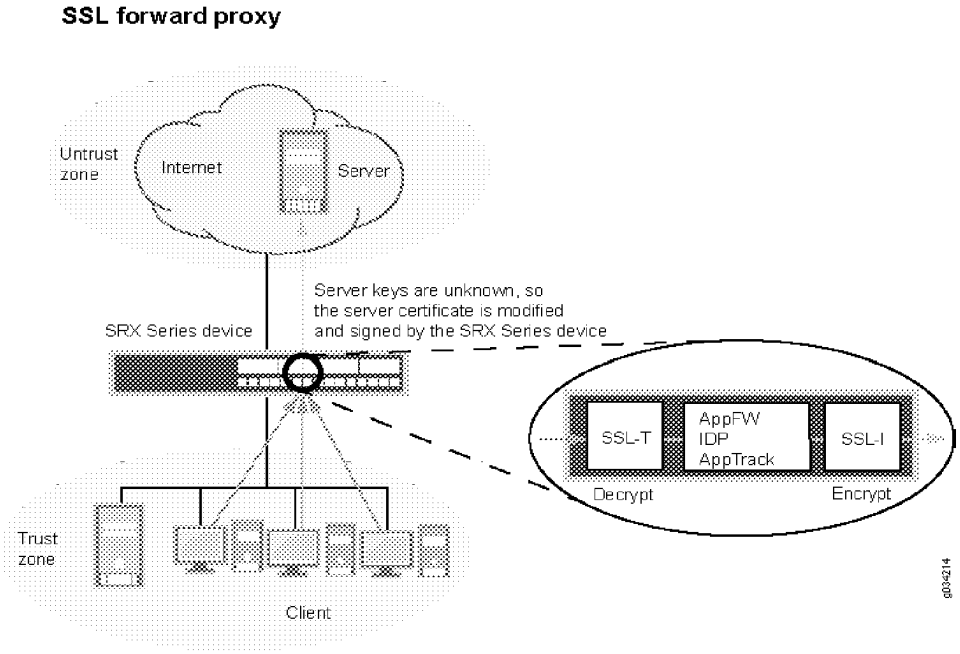
Figure 2 on page 13 shows how SSL proxy works on an encrypted payload. When application firewall (AppFW), Intrusion Detection and Prevention (IDP), or application tracking (AppTrack) is configured, the SSL proxy acts as an SSL server by terminating the SSL session from the client and establishing a new SSL session to the server, the SRX Series device decrypts and then reencrypts all SSL proxy traffic. SSL proxy uses the following:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.
- Configured AppFW, IDP, or AppTrack services use the decrypted SSL sessions.

NOTE: If none of the services (AppFW, IDP, or AppTrack) are configured, then SSL proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy.

NOTE: The IDP module will not perform its SSL inspection on a session if SSL proxy is enabled for that session. That is, if both SSL inspection and SSL proxy are enabled on a session, SSL proxy will always take precedence.

Figure 2: SSL Proxy on an Encrypted Payload



Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) is a feature of specific key agreement protocols that provides assurances your session keys will not be compromised even if the private key of the server is compromised. By generating a unique session key for every session flow a user initiates, the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key. For PFS to function, the key used to protect transmission of data must not be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material must not be used to derive any further keys.

The ECDHE (Elliptic Curve DHE) cipher suits are used to enable the PFS on SSL proxy. ECDHE cipher suits are based on elliptic curve cryptography, which provides the same level of security as the RSA with smaller keys. SSL proxy is targeted to support only ECDHE ciphers suites as they are less expensive computationally than DHE ciphers.