Managed Security Services – Enterprise

SERVICE DESCRIPTION

Allstream's Managed Security Service - Enterprise will implement and maintain a security solution that will protect the Customer's critical network resources. Allstream will provide consistent, dependable and high quality service that effectively utilises the expertise of Allstream's certified customer service representatives and security engineers.

FEATURES

Support. Allstream provides monitoring and technical support 24 hours a day,7 days a week with a guaranteed 30-minute response time. This means that within 30 minutes of contacting Allstream's support desk, a certified Allstream security specialist will be contacting the Customer's designated representative.

Monitoring. Allstream will monitor the Customer's security solution in order to: ensure all security devices are up and running; ensure all security software ("Software) and hardware ("Hardware") provided by Allstream (collectively, the "Security System") is functioning; and confirm the status of the Customer's Internet connection. If Allstream Is notified of a problem with the Customer's Security System, a Managed Security Service engineer will be alerted to investigate and fix the problem.

Monthly Reports.
Allstream will provide the Customer with

(i) a monthly report that will include the Customer's network infrastructure and the URL Filtering rule set (if the Customer has subscribed to Allstream's Managed URL Filtering Service);
(ii) a monthly report that will include Inbound traffic accepted & denied, outbound traffic accepted & denied, firewall audit, firewall CPU utilization reports, trouble ticket reports and a VPN client usage report (if the Customer subscribes to Allstream's Managed VPN service);
(iii) a quarterly vulnerability scan report of security devices managed under Allstream's Full Managed Security Service.**

Customers may have reed-only access into Firewall management system to review their firewall rules. Customers that subscribe to Allstream's Managed Anti-Virus service may have read-only access to their gateway anti-virus server to review anti-virus activity.

** Interpretation of vulnerability scan reports Is charged at Allstream's professional service rates

DOCUMENTATION OF NETWORK INFRASTRUCTURE.

As part of Implementing Allstream's Managed Security Service, Allstream will work with the Customer's designated representative to document the Customer's network infrastructure. Required information to be documented for Managed Firewall Service includes: IP addresses of all devices within the DMZs off of the Managed Firewall Service; a network diagram of where the managed firewall is located within the Customer's network; and IP address domain provided by the ISP or registered with ICCAN. Required information to be documented for Managed URL Filtering Service

includes: sub-nets within the Customer's network; and a network diagram of where the managed URL Filtering server is located within the Customer's network. Required Information to be documented for Managed Anti-Virus Service includes: a network diagram of where the managed anti-virus server is located within the Customer's network.

MANAGING AND MAINTAINING THE SECURITY SVSJEM.

In addition to the managing and maintaining the Customer's Security System in accordance with Allstream's Internet User Policy, Allstream protects against new vulnerabilities as follows:

- Updates and Patches - On an ongoing basis, Allstream will: ensure the Customer's Security System is up to date by installing required updates and patches. Updates and patches will be classified by Allstream into four categories:

- Critical - There is real and imminent danger of intrusion causing serious damage if the Software is not updated. The update will be installed on the Customer's relevant Security System devices within 24 hours of being informed of the update by the software manufacturer. If the Customer has not subscribed to Allstream's high availability service for the relevant Security System device, the Customer may experience Service down time during the Software upgrade. Service down time due to critical Software upgrades will be excluded from any calculation of availability for the purposes of the Availability Guarantee. Allstream will contact the Customer's designated representative within 12 hours of being notified by the software manufacturer. Updates will be carried out upon approval by Allstream's VP of Customer Services.

- Important - There is danger that, without this patch, the Customer will be vulnerable to an intrusion that may cause serious damage. The update will be installed on the Customer's relevant Security System devices in the next appropriate maintenance window. Allstream will provide a minimum of 2 weeks notice before an update.

- Not important - There is danger that without this patch, the Customer will be vulnerable to intrusions that would cause irritation but no serious damage. The update will be installed on the Customer's relevant Security System devices as a part of a general upgrade in order to maintain Software image consistency within the Managed Security Service. Allstream will provide a minimum of 2 weeks notice before an update. Allstream will do the update during a standard maintenance window.

- Not Relevant - The patch or update is not relevant to the Customer's network environment. At the sole discretion of Allstream, the update may be installed on the Customer's relevant Security System devices as a part of a general upgrade in order to maintain Software image consistency within the Managed Security Service. Allstream will provide a minimum of 2 weeks notice before an update. Allstream will do the update during a standard maintenance window.

- Rules Changes - Allstream will complete rule changes requested by the Customer or suggested by Allstream's security engineers. Twenty rule modifications per Security System device per month (including additions and deletions) are included in the Managed Security Service.

The Customer may choose to pay a lower monthly price by opting to have a fewer number of rule changes each month as set out below:

Checkpoint SOHO license: Maximum of 5 rule changes each month.
Checkpoint Enterprise license: 20 rule changes per month during the initial three months of the Term, and maximum of 5 rule changes each month for the remainder of the Term.

When the Customer requests a specific rule change, the Customer is responsible for ensuring the change does not introduce vulnerabilities in the Customer's network. Rule changes will be

implemented at a rate of no more than 4 hours per rule from the time the rule change request is submitted to Allstream. An Allstream security engineer will contact the Customer's designated contact person within 30 minutes of Allstream receiving the rule change request. When the Customer requests a specific rule change, the Customer is responsible for ensuring the change does not introduce vulnerabilities in the Customer's network. Any requests for Allstream to install a new web page will constitute a rule change.

- ❑ Software Subscriptions - Allstream will track and renew the software subscriptions for the Software under Allstream management.

- ❑ Customer Information Back-ups - Allstream maintains back up logs, policies, and configurations to ensure the most current configuration is readily available. Five previous generations of policies and configuration will be archived. Policies and configurations will be backed up within 24 hours of a policy or configuration change. Logs will be provided to the Customer via e-mail or be sent out by courier on CD(s) within 2 business days of request. A maximum of 12 requests may be submitted per year.

- ❑ Archive Logs - Archive logs will be archived for one year. Archiving will be done every 24 hours. The list of logs that will be archived are as follows:

    - For Managed Firewall/VPN Service: System Logs and User Activity Logs
    - For Managed Anti-Virus Service: System Logs and Virus Detection Logs
    - For Managed URL Filtering Service System Logs and URL Filtering Logs

- ❑ Hardware Failure - In the event that the Hardware, located in Canada, fails and Allstream is not able to resolve the problem remotely, Allstream will ensure replacement hardware is delivered to the courier the next business day for overnight delivery.

- ❑ Key Management - Allstream will, on a quarterly basis, refresh the encryption key on the VPN gateways for Site-to-Site VPNs where both ends of the VPN tunnel are managed by Allstream. Allstream will, on a quarterly basis, refresh the encryption key between the VPN gateway and the radius server, both of which are managed by Allstream.

- ❑ VPN tunnels between VPN gateways managed by Allstream and VPN gateways not managed by Allstream - Allstream will provide to the person managing the VPN gateway and setting up a VPN tunnel to an Allstream managed VPN gateway, the IPSec settings that will enable a proper VPN connection to Allstream's managed VPN gateway. Allstream will ensure that the corresponding IPSec setting is configured on the Allstream managed VPN gateway. Allstream will ensure that the configuration provided is in compliance with Internet Engineering Task Force approved IPSec standards. Allstream cannot ensure that a successful VPN connection can be made if the VPN gateway to which Allstream is connecting to is not fully IPSec compliant.

- ❑ VPN Client Software Support - Allstream provides 7x24x365 telephone support of the Software. The 2nd level support is provided:
    - Allstream2nd Level Support means that only the Customer's help desk administrators may contact Allstream's help desk for support
    - Allstream's Professional service charges may apply for integrating the Customer's radius server with Allstream's Managed Security Service Remote Access Internet VPN Service.

- VPN Client Software Distribution - The Customer is responsible for the distribution and installation of the Software. Allstream will provide 2nd Level Support. Recommendations on Software distribution strategies may be provided as part of Allstream's Professional Services and will be charged in accordance with Allstream's professional services rates.

- Administrator's Guide - Allstream will provide the Customer with a Managed Security Service Administrator's Guide. The guide will include: an installation and user's guide for the Software as it pertains to Allstream's Managed Security Service; security policy guidelines; and a 1st Level Support Software troubleshooting guide. A customised security policy may be provided to the Customer and will be charged at Allstream's professional service rates.